ANALYZING NON-FUNCTIONAL CAPABILITIES OF ICT INFRASTRUCTURES SUPPORTING POWER SYSTEM WIDE AREA MONITORING AND CONTROL

Moustafa Chenine

March 2013

Submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy

Industrial Information and Control Systems
School of Electrical Engineering
KTH, Royal Institute of Technology
Stockholm, Sweden
ABSTRACT

The strain on modern electrical power systems has led to an ever-increasing utilization of new information and communication technologies (ICT) to improve their efficiency and reliability. Wide area monitoring and control (WAMC) systems offer many opportunities to improve the real-time situational awareness in the power system. These systems are essentially SCADA systems but with continuous streaming of measurement data from the power system. The quality of WAMC systems and the applications running on top of them are heavily, but not exclusively, dependent on the underlying non-functional quality of the ICT systems.

From an ICT perspective, the real-time nature of WAMC systems makes them susceptible to variations in the quality of the supporting ICT systems. The non-functional qualities studied as part of this research are performance, interoperability and cyber security. To analyze the performance of WAMC ICT systems, WAMC applications were identified, and their requirements were elicited. Furthermore, simulation models capturing typical utility communication infrastructure architectures were implemented. The simulation studies were carried out to identify and characterize the latency in these systems and its impact on data quality in terms of the data loss.

While performance is a major and desirable quality, other non-functional qualities such as interoperability and cyber security have a significant impact on the usefulness of the system. To analyze these non-functional qualities, an enterprise architecture (EA) based framework for the modeling and analysis of interoperability and cyber security, specialized for WAMC systems, is proposed. The framework also captures the impact of cyber security on the interoperability of WAMC systems. Finally, a prototype WAMC system was implemented to allow the validation of the proposed EA based framework. The prototype is based on existing and adopted open-source frameworks and libraries.

The research described in this thesis makes several contributions. The work is a systematic approach for the analysis of the non-functional quality of WAMC ICT systems as a basis for establishing the suitability of ICT system architectures to support WAMC applications. This analysis is accomplished by first analyzing the impact of communication architectures for WAMC systems on the latency. Second, the impact of these latencies on the data quality, specifically data currency (end to end delay of the phasor measurements) and data in-completeness (i.e., the percentage of phasor measurements lost in the communication), is analyzed. The research also provides a framework for interoperability and cyber security analysis based on a probabilistic Monte Carlo enterprise architecture method. Additionally, the framework captures the possible impact of cyber security on the interoperability of WAMC data flows. A final result of the research is a test bed where WAMC applications can be deployed and ICT architectures tested in a controlled but realistic environment.

Key words: Power System Communication, Wide Area Monitoring and Control systems, Phasor Measurements Units, Power System Communication, SCADA systems.
ACKNOWLEDGEMENTS

A lot of people have contributed to this work, directly and indirectly. My deepest gratitude goes to my supervisor Lars Nordström and co-supervisor Pontus Johnson for all their continuous support, encouragement, enthusiasm and patience throughout the PhD work.

I would also like to thank Torsten Cegrell who gave me a chance to start on the PhD and for getting me interested in the topic area from the first interview. A special thanks to Judith Westerlund and her family. Thank you for welcoming me into the department, making sure I was never left out and always making me feel at home.

I would like thank present and past colleagues at ICS for the stimulating and rewarding environment throughout the years, Mathias Ekstedt, Joakim Lilliesköld, Robert Lagerström, Mårten Simonsson, Per and Pia Närman, Johan Ullberg (and for all the advice on adjusting in Sweden and the countless lost in translation assistance!), Teodor Sommestad, Kun Zhu, Johan König, Ulrik Franke, Markus Buschle (and for being a tech news nerd like me), David Höök, Nicholas Honeth, Arshad Saleem, Hannes Holm, Waldo Rocha Flores, Evelina Eriksson, Magnus Österlund, Yiming Wu, Khurram Shahzad, Liv Gingell, Annica Johannesson, Davood Bahazadeh, Shahid Hussain and all the other wonderful colleagues at ICS, it has been a pleasure working with you all.

A special acknowledgement also goes out to my co-authors, some of whom are listed above, thank you for working with me on the various projects throughout the years, and special thanks for Kun Zhu for continuous constructive discussions on the subject matter.

I would like to thank the folks at Swedish National Grid (Svenska Kraftnät), Dr. Göran Ericsson, for his support and encouragement, and Mr. Sture Holmström for his support and enthusiasm and from whom I have gained valuable practical knowledge while working with him. I would also like to thank all the other folks at the Relay Protection and Power System Data department for their warmth and curiosity.

My licentiate and doctoral work were both supported by the ELEKTRA program, their financial support is greatly appreciated.

Finally and most importantly, my deepest gratitude goes out to my family: My father, Ahmad, mother, Najibe, brother, Mohammed, my little sister, Sarah, and my wonderful wife Zakiya and our children Ahmad Jonas and Safwan Adam. Thank you for your understanding, support and encouragement ever since I started on this journey.

Moustafa Chenine
Stockholm, February 2013
LIST OF INCLUDED PAPERS


Author Contributions

In Paper A, the general research concept and authoring was due to Chenine with Nordström providing support.

In Paper B, the general research concept was due to Zhu, Chenine and Nordström, Chenine contributed to the communication simulations, and advice on implementation of the experiments and presentation of the results for which Zhu was the primary contributor. Authoring was primary done by Zhu with major contributions from Chenine.

In Paper C, the project scope and delimitation was set by Chenine, implementation was performed by Ivanovski, Maden and Chenine, Nordström and Al Khatib provided guidance and input, authoring was performed by Chenine and Al Khatib.

In Paper D, the primary contributions and authoring was due to Chenine and Vanfretti, where Chenine, implemented the online system and Vanfretti provided algorithms for Mode Estimation, Nordström provided valuable contributions on the architecture and vision. Bengtsson contributed to the offline applications implementation.

In Paper E, the primary research concept, implementation and authoring was due to Chenine, Ullberg and Nordström, Yiming provided valuable related research, and Ericsson provided valuable input and structuring on the model and implementation.
LIST OF PAPERS NOT INCLUDED IN THE THESIS

Publication I 

Publication II 

Publication III 
Yiming Wu, Kun, Zhu, Moustafa Chenine and Lars Nordström. “Framework Incorporating Synchronized Phasor Data For Power System Operation and Control”. In the 9th IET International Conference on Advances in Power System Control, Operation and Management (ASPCOM), Hong Kong, 2012.

Publication IV 

Publication V 

Publication VI 

Publication VII 

Publication VIII 

Publication IX 

Publication X 

Publication XI 

Publication XII 


# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTRODUCTION</td>
<td>3</td>
</tr>
<tr>
<td>BACKGROUND</td>
<td>3</td>
</tr>
<tr>
<td>RESEARCH OBJECTIVES</td>
<td>4</td>
</tr>
<tr>
<td>RESEARCH RESULTS</td>
<td>5</td>
</tr>
<tr>
<td>THESIS OUTLINE</td>
<td>12</td>
</tr>
<tr>
<td>RESEARCH CONTEXT</td>
<td>13</td>
</tr>
<tr>
<td>POWER SYSTEM MONITORING AND CONTROL</td>
<td>13</td>
</tr>
<tr>
<td>POWER SYSTEM COMMUNICATION</td>
<td>15</td>
</tr>
<tr>
<td>INTEROPERABILITY</td>
<td>17</td>
</tr>
<tr>
<td>CYBER SECURITY</td>
<td>18</td>
</tr>
<tr>
<td>RESEARCH DESIGN</td>
<td>21</td>
</tr>
<tr>
<td>DATA COLLECTION</td>
<td>21</td>
</tr>
<tr>
<td>MODELING AND ANALYSIS</td>
<td>22</td>
</tr>
<tr>
<td>SUMMARY</td>
<td>27</td>
</tr>
<tr>
<td>RELATED WORKS</td>
<td>29</td>
</tr>
<tr>
<td>CONCLUSION</td>
<td>33</td>
</tr>
<tr>
<td>CONTRIBUTION</td>
<td>33</td>
</tr>
<tr>
<td>FUTURE WORK</td>
<td>33</td>
</tr>
<tr>
<td>BIBLIOGRAPHY</td>
<td>35</td>
</tr>
<tr>
<td>PART II: PAPERS A TO E</td>
<td>45</td>
</tr>
</tbody>
</table>
PART I: INTRODUCTION
CHAPTER 1

INTRODUCTION

This chapter provides a brief introduction to the research topic and the objectives of the research presented in this thesis. Then, the chapter provides a summary of the results of the research. Finally, the chapter closes with an outline of the thesis.

BACKGROUND

Modern electrical power systems are undergoing vast fundamental changes in terms of the portfolio of connected devices, systems and possible generation and electrical storage units. The driver behind the changes is a realization of the need to modernize the entire process and the supporting systems to achieve efficiency in terms of production, transmission, distribution and consumption of electrical energy. This need for efficiency, in turn, was born in an environment where new opportunities have become apparent (such as the availability of renewable energy production technology, wind, hydro, etc.) and where regulatory and environmental restrictions are in place. At the same time, the possibilities, such as the use of wind power and/or integration of distributed generation, introduce technical challenges for the security and reliability of the power system. To counter these technical challenges, modern information and communication technologies (ICT) are increasingly being utilized in every aspect of power system protection, automation, control and planning.

Traditional power system operation and control, has for decades, been performed with systems built in a centralized architecture, using supervisory control and data acquisition (SCADA) and energy management systems (EMS). These were built largely on proprietary systems and protocols. With the adoption of new technologies, power system operation and control is moving towards more decentralized and open architectures, systems and protocols [1], [2], [3], [4]. The current approach for power system operations at the transmission level is to perform most of the monitoring and control actions within an EMS, which makes use of data from a SCADA system.

SCADA/EMS systems have served well when sufficient security margins and reserves are taken, but, with the changing portfolio of generation, the increasing load and the interconnection of national grids, there is a need for more real-time dynamic monitoring and operation of the power system [5],[6],[7],[8],[9]. The main disadvantage with SCADA/EMS systems is the low sampling and update rate, which usually provides a steady state view of the power system and therefore is unable to fully account for power system transients such as oscillations [10], [11].

To meet these challenges, wide area monitoring and control (WAMC) systems\(^1\) are being deployed internationally [12], [13], [14], [15], [16]. Phasor measurement units (PMUs), the main enabler for WAMC systems, provide from the power system high-resolution sub-second frequency and phasor measurements that are time stamped using a high precision time source. This functionality allows dynamic real-time observation of the power system

\(^1\) There are several types of phasor based systems covering monitoring, and control and protection functions. In this thesis, wide area monitoring and control is used to refer to those systems that cover monitoring and control functions because the ICT system supporting them is essentially the same or similar.
states and enables a whole range of applications and methods that can be used to manage the system at a more efficient and responsive level than previously possible.

While PMUs have been around since the 1980’s, limitations in the supporting infrastructures and primarily the ICT infrastructure made the deployment of such systems infeasible. With the increased modernization of the power system and the supporting infrastructures driven by international initiatives and roadmaps [18], [19], [20], [21], [22], the role of ICT systems is increasingly being recognized as a critical component for the success of WAMC systems.

**Research Objectives**

WAMC systems are a promising solution that could facilitate the real-time operation and control of the power system, which would allow greater utilization of the transmission capacity in existing infrastructure and fast corrective responses in abnormal transient situations in the power system. As indicated in [23], [24], [25], [26], [27], [28], [29], [9] and more recently in [30], the performance of the WAMC systems is largely dependent on the performance of the ICT infrastructure that supports these systems, namely due to the high sampling rate in WAMC systems. If the ICT infrastructure is unsuitable and cannot meet the requirements of applications in WAMC systems, then these systems will not be as useful as intended.

Additionally, other important quality issues exist, which are also important in the context of an integrated and modern control system architecture. The increased integration of WAMC systems with other traditional power system management systems (e.g., SCADA/EMS) and the increase in the awareness of the importance of interoperability and cyber security in the power system domain has prompted an increasing interest in these two non-functional qualities. These issues have been partly addressed in efforts to integrate and interoperate with established communication standards for synchrophasors, exemplified in the mapping of IEC 61850 and IEEE C37.118 [33], among other initiative and works [35],[36]. The increased awareness of cyber security in the domain of power system management is also applicable to WAMC systems. There have been several initiatives and increased interest in determining what the main security concerns are in WAMC systems and how to assess such security concerns [34][35][36][37][38].

Taking the aforementioned issues into context, the following objectives were set for the research presented in this thesis:

- Investigate communication requirements that core applications of WAMC systems have and analyze the fulfillment of these requirements in various wide area communication architectures.
- Identify the impact of the ICT architecture on the data quality specifically, the currency and the completeness of the data and its impact on the WAMC application.
- Propose a framework to model and analyze the non-functional quality of WAMC system architectures, specifically focused on interoperability and cyber security.
- Implement a test bed for WAMC application testing, analysis and validation that enables validation of this framework.
RESEARCH RESULTS

The initial set of results as reported by this author in [39] was focused on architectural performance, with communication network architecture receiving the main bulk of the effort. This is because the communication network was viewed as the main bottleneck given the modern evolution of communication systems in utilities, where traditional propriety protocols of legacy systems determined the architecture of the overall system. This initial set of results can therefore be split into two categories, namely application requirements and WAMC communication and application modeling and simulation. As is apparent in [39], this work was presented in the licentiate thesis of the author and forms an important platform for the remainder of the work.

The architectural analysis of WAMC systems is the next important component of this research, where enterprise architecture methods were adopted and specialized to model concepts in this field. The modeling was focused on the interoperability and cyber security aspects of WAMC systems. Finally, given the high performance and critical features of WAMC systems, a test bed was developed for future application testing and analysis, which was accomplished by using industry standard open-source systems to build a platform where WAMC applications can be hosted.

The remainder of this section provides a summary of the results.

PERFORMANCE AND COMMUNICATION SIMULATION

The first objective of this research was to investigate the communication requirements of core applications in WAMC systems and to analyze the fulfillment of these requirements given different communication architectures and characteristics. The latter can be further specified as the analysis of the latency characteristics in the ICT systems that support WAMC systems to understand the impact of the latency on the overall quality of the WAMC system applications. Paper A describes the process that was used to do so and the results obtained at each stage.

From an ICT perspective, some baseline requirements have to be established to say anything about the performance or the architecture. Therefore, the first stage of this research aimed at consolidating WAMC requirements as understood by researchers and practitioners in the Nordic region at the time and compared to similar requirements on WAMC applications [40] prepared by the North American Synchrophasor Initiative (NASPI) [22]. In terms of WAMC application requirements, the survey queried the participants on the current stage of development and implementation of WAMC systems. The survey also collected prioritizations for WAMC applications from the participants. These prioritizations represent the degree of importance the participants attached to the applications, given the characteristics of their respective power systems. The most important outcome of the survey was, however, a set of ICT requirements for WAMC applications. A more detailed discussion on the Nordic WAMC application requirements survey can be found in Publication XVIII.

The requirements considered aspects of the applications such as the data resolution or the network delay tolerable for the measurements from the remote PMUs to reach the control center (specifically to be accessed by the application). An example of the requirements collected is depicted in Figure 1 below. The figure shows the requirements for the oscillation detection application. These requirements represent the opinion of participants who would apply these applications in an industrial setting.
The second stage aimed at building several possible WAMC communication network models and, using input from the survey, to gain a deeper understanding on how the characteristics of latency change given different system parameters (i.e., bandwidth, protocol, application settings, etc.). Using the initial delay results from these models and abstracting the WAMC system and the communication network enabled the general specification of delays experienced in WAMC systems, which was accomplished by studying the impact of these delays on the phasor data concentrator (PDC) and elaborating its parameters, such as the waiting time limits and data loss that may occur if these limits were introduced. The waiting time limits at the PDC determine the maximum delay that can occur on the network and are a direct result of the delay variations in the communication network between the remote PMUs and the control center. Examples of these results are shown in Figure 2, where various waiting times and associated data loss rates were used.

Figure 1: Example of output from survey, data for the Oscillation Detection Application Function

<table>
<thead>
<tr>
<th>Interviews</th>
<th>Expected Latency</th>
<th>Expected Resolution</th>
<th>Expected Time Window for Response</th>
<th>Format/Protocol</th>
<th>Time Delay for Current/Extending Control Schema</th>
<th>Expected Execution Time for Control Schema</th>
</tr>
</thead>
<tbody>
<tr>
<td>TSO 1</td>
<td>10 Hz</td>
<td>Less than 0.3 seconds</td>
<td>BEES 1544</td>
<td>To be determined</td>
<td>Wedge Offline/Offline</td>
<td></td>
</tr>
<tr>
<td>TSO 2</td>
<td>Less than 2 seconds</td>
<td>10 Hz</td>
<td>Functions of seconds</td>
<td>C37.118</td>
<td>Not applicable</td>
<td>Functions of seconds</td>
</tr>
<tr>
<td>TSO 3</td>
<td>0.25-2 or 3 seconds</td>
<td>100/50 Hz for online/offline applications</td>
<td>C37.118</td>
<td>0.25 seconds</td>
<td>0.25 seconds</td>
<td></td>
</tr>
<tr>
<td>Research Institute 1</td>
<td>Seconds</td>
<td>Seconds/Minutes for automated/manual control</td>
<td>Seconds</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Research Institute 2</td>
<td>Functions of seconds</td>
<td>Above 10 Hz</td>
<td>Less than 1/10 of the cycle time of studied oscillation</td>
<td>C37.118</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Research Institute 3</td>
<td>1 second</td>
<td>50 Hz</td>
<td>Less than 0.25/5 seconds for PDC/SPS</td>
<td>Less than 1 second</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NASPI</td>
<td>1-5 seconds</td>
<td>10 Hz</td>
<td>Seconds</td>
<td>PDC Schemes/</td>
<td>C37.118</td>
<td></td>
</tr>
</tbody>
</table>

Figure 2: ETE Delay and Data Incompleteness in a WAMC system with 8 PMUs
Figure 2 illustrate the delay and the data incompleteness of a WAMC system with 8 PMUs for normal or “Base” delay and delays that are above the normal level, labeled “Extended” in the figure. This work is also described in Paper A and in more detail in Publication XVI.

These results are a step forward in understanding the possibilities and limitations of WAMC systems. WAMC systems intended for centralized applications such as situational awareness require data from several separate locations within the power system. The simulations presented in this paper indicate that the geographic distances, the background traffic and the architecture of the WAMC system will have an impact on the delay and/or completeness of the PMU data provided to the applications at the central location. Depending on the configuration of the PDC (e.g., the waiting times and the time out configurations) and the characteristics of the network in terms of delay, some central applications may not receive data of a sufficient quality to provide useful support in transient situations. These configurations and characteristics also have a key role to play in determining the bottlenecks in the architecture. The actual use of the PDC model in the study is an important distinction from previous works in the field where the PDC was not taken into account or assumed to be an insignificant part.

The results on the delays and the data incompleteness were then applied to further demonstrate the dependency of WAMC applications reliability on the supporting ICT system architectures (see Paper B). This study generalizes the results and shows the consequence to the WAMC application of inappropriate architecture choices, which lead to insufficient data quality. In the study, a comprehensive analysis was performed on the reliability of a power oscillation damping function given different architectures that exhibit different delay profiles. Two scenarios were used: Architecture 1, in which the concentration was centralized, and Architecture 2, in which the concentration was local, next to the regulating device. Figure 3 summarizes the scenarios in the study.

Figure 3: Architectural scenarios used in the study and the corresponding results.
The study also points out the impact of the latency on the reliability of the application, not only due to the currency\(^2\) of the data but also due to the completeness of the dataset, given the effect the PDC configuration has on the data. The reliability can be defined as:

\[
\text{Reliability} = 1 - \sum_{i=1}^{n} P(T_{TO})^{i} 
\]

where

- \(P(T_{TO})\) represents the probability of data loss for each PMU given the time-out parameter \(T_{TO}\).
- \(T\) is the maximum delay, in seconds, tolerated by the SVC function.
- \(S\) is the data resolution, measured as samples per second.

The function above actually provides insight into the tradeoff between the latency (currency) and the data loss (incompleteness) given the threshold of a certain application, which is the maximum tolerated delay \(T\). However, this function is not complete because the sensitivity of the application to data loss has not been investigated, and other general applications could also include compensated data, i.e., calculated data or the previous data. Such sensitivity studies must also be carried out to define the reliability or robustness functions that can serve as an important basis to determine stringent performance requirements for applications.

WAMC applications such as the one described above, therefore require some sort of guarantees on the data quality, i.e., the latency or the data incompleteness. Traditionally and analogous to power system transmission planning, where over-capacity was embedded in the design and the deployment of transmission lines, for example, the same practice is applied to communication networks, in which networks are over-provisioned, providing more bandwidth and capacity. However, this approach is clearly not optimal, especially in traditionally best-effort (specifically TCP/UDP/IP) networks and more specifically when traffic can become sporadic and possibly lead to network resource contention.

To provide some sort of guarantee, quality of service (QoS) mechanisms [42] can be utilized. This was the next stage of the research, in which Resource Reservation Protocol (RSVP) and Multi-Protocol Label Switching (MPLS) configurations were simulated based on further specifications of network configurations at a Nordic transmission system operator (see Paper C). Various traffic types were identified and implemented in the simulation study, specifically those originating from PMUs, remote terminal units (RTUs), video streaming (for surveillance of substations) and IP telephony. Figure 4 illustrates the basic configuration for all simulation scenarios used. Based on this basic configuration, the scenarios were varied by changing the bandwidth and the QoS parameters. Two scenario sets were configured based on this set up, with one scenario set having no QoS while the other set had QoS. Each scenario set consisted of three scenarios in which the bandwidth was the investigated parameter.

\(^2\) Currency is an attribute of data quality that describes the state of the data due to latency, i.e., due to delay, the data no longer reflects the most updated representation of the physical quantity, see [41] for a discussion of data quality attributes.
An example of the results is shown in Table 1. The table shows that QoS mechanisms are fundamental for WAMC communication, specifically when an IP network is used for collecting measurements and communication with other types of devices not directly associated with the WAMC system. By prioritizing traffic, the network can be better provisioned to meet the demands of different applications. While QoS does not necessarily decrease the delay, as the bandwidth rises, it does decrease the data loss and thus improve the overall data quality of the WAMC system. Since the traffic is prioritized over others, the probability of data loss is lowered, which greatly increases the reliability of applications dependent on it.

Table 1: Summary of Simulation Results for QoS comparison

<table>
<thead>
<tr>
<th>Scenario</th>
<th>2 Mbit/s</th>
<th>4 Mbit/s</th>
<th>8 Mbit/s</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Latency</td>
<td>Packet Loss</td>
<td>Latency</td>
</tr>
<tr>
<td>Scenario Set 1</td>
<td>46 ms</td>
<td>69.4 %</td>
<td>10.6 ms</td>
</tr>
<tr>
<td>Scenario Set 2</td>
<td>12 ms</td>
<td>58.3 %</td>
<td>10 ms</td>
</tr>
</tbody>
</table>

WAMC APPLICATION ANALYSIS TEST BED

One of the limitations of performing research in this field is the lack of actual real world systems on which experiments can be conducted. An experimental WAMC system would serve as a platform for the validation of ICT systems for WAMC. Thus, a platform for WAMC system architecture and application analysis was developed as part of this research.

The PowerIT platform, described in Paper D, is composed of several components, most of which are open source. This has allowed experiments with different architectures and the building new monitoring and analysis applications, some of which were presented in Paper D. The advantages of this system are as follows:

- It helps to expedite research and development efforts within the field of wide area situational awareness in terms of algorithms implemented in practice using real data, which would otherwise be solely based on simulation results.
- The platform also helps in determine and evaluate the impact and limitations of ICT systems on the genuine reliability and usability of these algorithms, again...
this is done by implementing algorithms and evaluating their performance on real
data in a real-time fashion as opposed to off-line batch processing.

The PowerIT platform has been further expanded and included in studies that take into
account the end-to-end cyber-physical system, that is, the ability to study in real-time the
simulated process, the real or emulated interfacing devices, the communication network
and finally the application. This work has been described in later works, as shown in Publi-
cation V and Publication VI. These works are similar in the sense that both aim for an end-
to-end analysis of the power system and its ICT components.

**INTEROPERABILITY AND CYBER SECURITY MODELING**

While the performance and data quality related aspects of ICT systems for WAMC systems
are fundamental for their basic functionality, other non-functional qualities directly impact
the robustness of WAMC systems. There are clear interdependencies between the non-
functional aspects and the attributes of the ICT system that comprise them, see [43], [44].
In some cases, there is even a negative coupling, for instance, between interoperability and
cyber security.

An architecture-based analysis method was used to address these concerns. This approach
builds on previous work in the field of architecture analysis, specifically drawing on enter-
prise architecture analysis. The use of enterprise architecture (EA) models supported by a
formal framework for analysis is an approach to managing and optimizing complex ICT
systems and processes. EA analysis methods have been applied in many scenarios, for
example, in [45], [46],[47], and more specifically have been focused on the non-functional
qualities of power system or utility ICT architectures, applications and processes in subst a-

tion automation systems reliability [48], data quality [49], control system cyber security [50]
and interoperability[51].

The WAMC Analysis Meta Model (WAMM) framework (see Paper E) aims to model
WAMC systems from a multi non-functional quality perspective. Specifically, the fram e-
work aims to capture the cyber security and interoperability aspects of WAMC systems.
The models developed using the framework allow the user to perform analysis of several
WAMC system architecture scenarios from the perspective of the aforementioned non-
functional qualities, which will allow more informed decision making such as which aspects
of the system could be optimized or secured further and what implications these actions
would have on the interoperability and the performance.

The main component of the framework is a modeling language that captures concepts
related to WAMC systems. The framework is a specialization of more general frameworks
that consider interoperability [51]and cyber security [52].In [51], an interoperability perspec-
tive is utilized, where the modeling language is used solely to capture various information
system concepts that have a role in enabling interoperability. However, the model de-
scribed in [52] captures various concepts critical to analyzing cyber security in general. The
model contains information system concepts that are related to cyber security, such as
countermeasures, attacks, and threats. The framework proposed is a specialized version of
the interoperability framework and adds the ability to model certain type of attacks on
WAMC system. The attacks are mostly related to data disruption between the client and
the server, e.g., PMU and PDC, PDC and the application, etc. The framework also makes
use of the security profile for wide area monitoring, control and protection [34] prepared
by the Advanced Security Acceleration Projects for Smart Grid (ASAP-SG). It does so by
adopting the roles identified by the profile as the main concepts used in the framework for
modeling. Figure 5 illustrates the concepts and relations of the framework.
The WAMM model presented in Figure 5 contains basic classes that are intended to represent real world systems, entities and concepts. There are four main classes in the model that can represent the basic structure of a WAMC system. That is, WAMC Component, Dataflow, Network Zone and Network Interface. Using these basic classes, it is possible to establish where a WAMC component is located, what its role(s) are, i.e., server or client, and the data flows it receives or transmits.

The WAMC Component class is a general class that can be used to represent various types of components and systems that can be associated with WAMC systems, for example, a WAMC Component can be further specialized to represent a PMU or a PDC.

![Figure 5: The WAMM Model](image)

Figure 6: Specializations of the WAMC component and Data flow Classes.
Figure 6 illustrates some specializations of the WAMC Component class that are relevant to WAMC systems, these specializations are mapping of concepts outlined in the ASAP-SG Wide Area Monitoring Protection and Control Security Profile [34].

This is also the case for other classes in the model, for example, Dataflow can be further specified to represent more concrete representation, i.e., a PMU Dataflow that represents a flow of measurements from a PMU vs. a PDC Dataflow, which represents a concentrated flow of measurements from a PDC. The attributes of the classes represent aspects or properties of the system that are of importance in performing interoperability or cyber security analysis. For example the attribute dropsMessage belonging to the WAMC Component, represents that a WAMC Component drops or discards data (due to, for example, faulty setup or an improper configuration, such as setting an unsuitable time source). All attributes in the model are Boolean and can be have a Boolean value, true or false, or defined in the form of a Bernoulli distribution.

In terms of cyber security, the framework is concerned with the confidentiality, integrity and availability of the data flow between roles, i.e., between the PMU and the PDC or between the PDC and the WAMC application that processes the data. These are assessed as a result of attacks on these data flows, e.g., disrupt attack renders the dataflow unavailable while an eavesdropping attack breaches the confidentiality of the data flows.

The modeling language is defined using the Predictive, Probabilistic Architecture Modeling Framework (P²AMF) [53], [54], which utilizes a probabilistic Monte Carlo approach and is further implemented in the Enterprise Architecture Analysis Tool [55].

**Thesis Outline**

The rest of this thesis is structured as follows. Chapter 2 provides a more detailed overview of the research context, describing contemporary control system architectures based on SCADA and EMS systems and giving an overview of power system communication systems, interoperability and cyber security. Chapter 3 is a brief description of the methodology that was used to implement the research described in this thesis. Chapter 4 describes related simulation work and other modeling approaches related to the study of WAMC ICT systems. Chapter 5 concludes this thesis, explicitly pointing out the contribution of the research and discussing future works. Part II of this thesis includes the Papers A – E, which were described in the results section of this introduction.
CHAPTER 2

RESEARCH CONTEXT

This chapter provides the background to the topic of WAMC systems. Specifically, the chapter provides an overview of SCADA and EMS functions as well as WAMC systems, their components and application functions.

POWER SYSTEM MONITORING AND CONTROL

It is often stated that electrical power systems are critical and vital infrastructures for the continuity of modern industrial and post-industrial societies. Likewise, ICT systems are the critical and vital infrastructures that make modern power systems possible and manageable.

Power system operation has since the early years, utilized some sort of automation system to monitor and control the power system. The earliest power control systems were based on electromechanical systems that were used for a small number of simple monitoring and control points [1], [56], [58], [59], [57]. With the advent of evolving ICT systems, it has become possible to collect large amounts of measurements and indications and present these data at a centralized location. At the centralized location, the collected information would be used by operators to evaluate the state of the power system. The information would also be used in applications for further contingency analysis, and, based on the judgments made by the operators or results from the applications, commands may then be sent out to remote actuators to change the state of the process.

SCADA SYSTEMS

The systems that are used to assist in managing a process of any size must have a simple set of functions:

- **Data Acquisition:** This functionality involves collecting data from remote/local devices to a central location, e.g., a central online database [59].
- **Monitoring:** This function monitors the incoming/stored data and compares them to previously received data or to limits set by the operators. The monitoring function also raises alarms to operators that certain limits have been reached or certain values have changed. For example, a change in the voltage level beyond a pre-set threshold would generate an alarm to inform the operator. In some cases the monitoring function may raise an alarm and automatically call on control functions to be executed [59].
- **Control:** The system also has the functionality to execute control functions. These control function change the state of the process by changing the state of remote devices. Opening or closing breakers or switches is an example of a control function [59].

Such systems are called Supervisory Control and Data Acquisition (SCADA) Systems [56], [1], [57], [58]. As SCADA is employed in diverse industrial processes, these systems have specific functionality related to the industry to which they are applied; in the case of electrical power systems, this extra set of functionality is called energy management systems (EMS) [60].
ENERGY MANAGEMENT SYSTEMS

While SCADA systems perform the routine collection of data, and sending of control signals, the actual functionality that is used to operate the power system is provided by EMS systems. These systems are actually suites of applications that run on top of the SCADA functionality to process and compute relevant information from the data that is collected. This information aids in the safe and reliable operation of the power system because it provides the operator with filtered and processed information from the power system. The foundation of the EMS applications is power system state estimation.

In power system state estimation the current state of the power system is determined. The state is based on the measurements (e.g., voltage and power flow) and digital values (e.g., breaker states) collected by the SCADA system. In some cases, these data may not be available from all parts of the power system or may be distorted or erroneous. The state estimator calculates the estimates of all states, normally voltages and phase angles, at all buses using the data provided by the SCADA system [60]. Other EMS applications use this power system state information, an example of such an application is Optimal Power Flow (OPF). In OPF, several hypothetical scenarios are calculated by varying the system parameters, which is usually done for particular criteria, for example, cost of generation or transmission line losses, and allows the operators to analyze the best scenario that meets the load conditions [61] and at the same time minimizes losses.

For a more in depth discussion on SCADA/EMS evolution, architecture and functionality see [1], [56], [58], [59], [60].

WIDE AREA MONITORING AND CONTROL SYSTEMS

In the late 1980s, the concept of phasor measurement units (PMUs) was introduced. This device can measure the voltage and current phasors as well as the frequency at a high sampling rate, while the measurements can be time-stamped by clocks synchronized via GPS satellites. This functionality is similar to disturbance recorders. It was first suggested that PMUs could be used to improve power system observations, for example, by improving state estimation [5], [6], [62], [63]. It was also recognized that the communication infrastructure limitation hindered the deployment and therefore usability of PMU technology [9], [24]. The importance of PMU based applications came to attention after the events of the 2003 blackout in the U.S and Canada [65], where the experimental system deployed showed that they did provide earlier situational awareness before the cascading event occurred.

PMUs are designed to measure the analog AC waveforms of the positive sequence voltage and current phasors at very high measurement rates, up to 60 measurements per second. In contrast, conventional RTU measurements are sampled every 10-60 seconds depending on the system configuration. Accordingly, this advancement makes PMUs a suitable tool to capture power system dynamics. In addition to phasors, PMUs are also capable of measuring the system frequency. The GPS signal is used to provide a time stamp for each measurement using coordinated universal time as the reference. For analogue to digital conversion, a discrete Fourier transform is applied to estimate the fundamental frequency components of the measured analog signal given samples taken at appropriate intervals[7][64]. Figure 7 illustrates the typical modules that compose a PMU.
A complete PMU based monitoring and control system is a system in which PMU measurements are collected from various locations in the electrical grid and the measurements are communicated to a central location, where they are used by an assessment or monitoring application that raises alarms or calculate results. The alarms raised and the results calculated by these monitoring systems are in turn used to provide corrective actions or control on the power grid. Such a complete PMU based system is known as a WAMC.

A WAMC system includes four basic components: a PMU, a PDC, the PMU-based application and finally the communication network [67]. Logically, there are three layers in a WAMC, which in essence are very similar to more traditional SCADA systems. Figure 8 illustrates the logical architecture of WAMC systems. Layer 1, where the WAMC system interfaces with the power system on substation bus-bars and power lines is called the Data Acquisition layer. Layer 2 is known as the Data Management layer, and it is where the PMU measurements are collected and sorted into a single time synchronized dataset. Finally, Layer 3 is the Application Layer, which represents the real-time PMU based application functions that process the time synchronized PMU measurements provided by Layer 2.

An in depth discussion of various architectures and communication systems for WAMC systems can be found in [25], [66] [67], [68] [76], [75].

**POWER SYSTEM COMMUNICATION**

Communication systems in power system operation and control typically contain a mixture of technologies and protocols. There are several factors that determine the characteristics of power system communication networks, some are related to the criticality of the pro-
cess, i.e., the need for reliable communication, and others are related to the organizational operation of the system, i.e., regulated and de-regulated [59], [69], [70].

The reliability of the communications was a driving factor in early power system communication, which, coupled with the limitation of early communication technology, can be observed in the design of early communication protocols such as DNP, Modbus, IEC 60870-101 [58], [59]. Early computer and communication systems had limited capacity in terms of processing power and storage space for the computer systems and bandwidth and communication media for the communication system. This limited capacity led to various communication techniques to manage and coordinate the multitude of available measurement points and status indications that can be made available from the power process.

Techniques such as polling and unbalanced polling [59] were introduced into the SCADA system and their protocols to manage the data from the process in a deterministic and efficient way. These techniques evolved as new communication technologies were introduced, especially with the introduction of Internet Protocol (IP)-based technologies [69]. The evolution did not eradicate the decades of well-established communication principles in power system and SCADA communication. In fact, these principles still exist and are applicable today, for example, IEC 60870-5-104 was introduced to make IEC 60870-5-101 compatible with IP communication [58]. However, the results are communication systems composed of heterogeneous techniques, media, protocols, and protocol converters with long-term investments in them. The following figure provides a hypothetical example of a typical utility communication network.

![Figure 9: A hypothetical power system communication network.](image)

While the IP suite was designed originally for the ARPANET, IP-like systems were employed in power systems communication at approximately the same time [71], [72]. The use of IP in power system communication was seen as an opportunity for increasing scalability, and improving quality of service [69] and seen as the de-facto communication protocol suite to alleviate the industry from proprietary protocols and to simplifying management.
However, the IP suite is also a cause for concern, primarily due to performance, predictability and security (with the use of the Transport Control Protocol) [75].

Synchrophasor-based system communication depart from traditional SCADA communication. The fundamental difference is, as mentioned earlier, that PMUs generally stream data continuously from source to destination, which is especially the case for centralized situational awareness systems (but not the rule) but can vary in distributed control, where a publish-subscribe paradigm can be employed. In fact, various schemes for synchrophasor communication over IP have been proposed, which can be seen in frameworks such as Gridstat [76], [77] and NASPInet [78].

Synchrophasors have also seen a proliferation of protocols, both proprietary and then standardized, for example, the BPAstream for concentrators, IEEE 1344[79], C37.118:2005[80], C37.118:2011. Strictly speaking, these protocols are more format definitions than full scale SCADA protocols, such as IEC 60870-5, and are meant to be communicated over the IP suite, serial connections or Ethernet. The need to harmonize different protocols and standards has also been recognized, for example, the harmonization of IEC 61850 and C37.118 [33], [83]. This harmonization is due to the increase of synchrophasor functionality available in devices other than PMUs, for example, in intelligent electronic devices (IEDs).

**INTEROPERABILITY**

Power system monitoring and control applications are increasingly composed of functions provided by multiple vendors or over various deployment phases. Interoperability among systems from various vendors enables easier information exchange, which in turn leads to increased business and operational efficiency. Furthermore, the use of standard off-the-shelf ICT systems has decreased operational costs [19]. In parallel to the developments of WAMC systems, information system models are being created to facilitate the integration and interoperability of SCADA/EMS and substation control systems. The prime examples of these developments are the standards being developed within IEC TC57 on Power System management and related information exchange [84], [85]. Within this committee, work is in progress regarding the applicability of state of the art information systems technologies such as service oriented architectures (SOA) for use in the implementation of, e.g., WAMC [86].

The National Institute of Standards and Technology (NIST) in the USA have also adopted the SOA approach for integration and interoperability in the smart grid. The NIST framework and roadmap for smart grid interoperability standards [87] describes the current status, issues, and priorities for interoperability standards development and harmonization. The NIST report also provides a high-level architecture for the smart grid, including a conceptual model, architectural principles and methods.

Furthermore, Cigré has also addressed the interoperability issue, albeit limiting its focus specifically on future EMS architectures [19]. Cigré’s initiative provides several architecture guidelines to enhance EMS and related application interoperability, specifically providing guidelines for information and integration architectures. The information architecture describes the business constraints and how the information flows throughout the system is mapped, for example, to the Common Information Model (IEC 61970-301) [84]. The integration architecture guidelines describe the design principles and the components for future architectures, including an integration layer. The integration guidelines describe how
components and functions are to operate in the system using the service oriented approach while meeting control room requirements such as performance and availability.

All of the above initiatives are developed in an engineering environment driven very much by specific industry needs. As a result there are several areas of overlap and “blank” areas in which standards are not being developed. In fact, systems built according to the propositions from these initiatives do not automatically become interoperable. In the scientific community, there are a few methods available for assessing interoperability implementations [87]. However, none address real-time systems for the power domain. Examples of frameworks for assessing interoperability can be found in [54], [88], [89], [90].

In the context of WAMC applications, the need for interoperability has been outlined in [18]. The importance of interoperability has become even more apparent when, as mentioned earlier, synchrophasor functionality is integrated with other power system monitoring and control devices, such as IEDs [91], which has led to harmonization efforts, for example, in [33] and the renewal of the main C37.118 protocols to specify both synchrophasor data formats and precision requirements in C37.118.1[81] and methods and format for exchange in C37.118.2 [82].

**Cyber Security**

Heterogeneous distributed systems introduce many concerns in terms of the confidentiality, the integrity and the availability of the information and data exchanged between these systems. There has been several standards proposed for information security in power system operation and control. These standards cover best practices or offer recommendations on managing and implementing security into monitoring and control systems or processes related to these systems. Some standards have already been selected for smart grid architectures by NIST [18], [35], for example, in [92], [93], [94]. NIST has also recently published a report on cyber security strategy and requirements for the smart grid [35]. The NIST report discusses security use cases for the smart grid and also includes use cases for WAMC systems (under Wide Area Situational Awareness). Cigré also provides security architecture for future EMS architectures. Cigré’s guidelines cover security in such areas as communication network segmentation, perimeter protection, centralized auditing and monitoring [19].

Guidelines for synchrophasor-based system have also been proposed, for example, the ASAP-SG [95] has established guidelines for several ICT platforms in the smart grid, one of which is the security profile for distributed management system [96]. The ASAP-SG also has a profile for Wide Area Monitoring Control and Protection [34]. These guidelines and other studies [35][36][37][38][98] have established the concepts in WAMC systems related to security and the possible sources of security uncertainty in regards to the characteristics of WAMC systems. While WAMC systems are prone to the same security concerns as other SCADA and power system automation systems, there are certain characteristics that are more common in WAMC systems. For example, the continuous stream of measurements and the requirements by applications to act on these data in short time frame requires the data quality to be high and the timestamps to be correct. If the data have been tampered with or the GPS time signal jammed [98], [99], can lead to disruption in the WAMC system, where data are no longer trusted. This situation can have more adverse effects on distributed control and protection applications, where the time frame for firing up such functions is short and the effects are immediate [99].
The limitation with these standards and best practices is that they are useful only as guidelines for implementing security, or the specification of protocol level security, but do not offer an opportunity to determine the level of security or to manage the effectiveness of the security measures implemented. To meet these challenges, researchers have developed methods for assessing and analyzing the security of these systems using quantitative approaches, for example in, [101], [102].
CHAPTER 3
RESEARCH DESIGN

This chapter discusses the processes and methods used in the research. The chapter begins with an overview of the research process and then discusses the methods for data collection, such as literature review, survey and expert input and validation. The next section discusses the analysis methods available. Simulation was the main analysis and experimental method that was selected, but enterprise architectural analysis methods were also employed and are discussed.

OVERVIEW

There are several methods that can be employed in a research project. These methods can include running experiments, running surveys, studying archival data, studying historical events, and finally studying a select set of case studies [103],[104]. There are different features for the method selected, how much control a researcher has on the method and the data collected and whether this method yields results that can take into account contemporary events.

This research has employed a combination of these methods for data collection to build models that represent the real world systems under study and analysis techniques for studying such models. Most of the models built were simulation models implemented on discrete event simulation tools. Discrete event simulations (DES) [105] are well suited for most ICT related performance analysis. For other non-functional qualities, DES may not be well suited, specifically interoperability and cyber security, in which case, system architecture analysis methods from the domain of enterprise architecture supported by Monte Carlo simulation were used.

DATA COLLECTION

The research in this thesis utilized two methods to collect data. First, data collection was executed through a literature review, followed by a survey of a specific focus group. Some participants of the survey were interviewed, others filled in the survey without an interview. The results of the literature review and the survey were then applied as input for building the simulation models. The amount of data collection was highly concentrated at the start of the research and gradually decreased as the models and simulations were built.

LITERATURE REVIEW

As mentioned in Chapter 2, there has been similar work in the field by other researchers, industrial working groups and standards. The characteristics of these literature sources vary, for example, literature sources from the academic community usually describe a hypothesis, experiments and results from predominantly controlled studies. The review of this literature formed the basis for initial model characteristics and assumptions in this research. The literature review was important in the sense that it led to a survey and to the selection of the focus group for the survey.
SURVEY

The survey was conducted using interviews and questionnaires. The questionnaire was composed of thirteen questions sent out to transmission system operators (TSOs) and researchers involved or planning to be involved in PMU project implementations. The survey was conducted both online, by use of email, and using face-to-face interviews conducted on the premises of the TSOs/researchers.

The questionnaires were semi-structured to guide the participants through the relevant topic areas, but sufficiently flexible to allow the participants to provide insight into their opinion. Interviews were also conducted with participants, in which case the contents of the questionnaire were used as the main agenda of the interview. This work is documented in Paper A and more completely in Publication XVIII.

Data were also collected from experts as input to simulation models or for the verification of simulation models. For example, data from the survey were used in Paper A and Paper C to build a preliminary communication network based on PMU locations, and the actual characteristics and properties of the final network model were verified with experts who were not survey participants. The algorithm for the PDC, described in the Paper A and B, was derived from literature but then validated with two experts that had developed or had worked with PDCs.

MODELING AND ANALYSIS

There are two basic categories of methods for ICT system evaluation. These are (1) measurements of existing systems and (2) predictions based on models that abstract existing or upcoming systems [105], [106], [107]. The first method, involves having a real world system to study, which would be at the disposal of the researcher to change environmental variable to observe the outcome. The types of ICT systems studied in this research, that is, infrastructure systems, make this method impractical and prohibitively expensive to carry out.

The second category involves modeling the system, replicating or simplifying key components and attributes of the system and studying these models for prediction. This category can further be split in two closely related evaluation processes, that is, analytical modeling and simulation modeling.

In this research, both methods were applied for modeling and analysis. Simulation methods were used primarily for the performance analysis of communication systems (Paper A, B and C), and analytical modeling using enterprise architecture methods was used to model the WAMC system as a whole for interoperability and cyber security analysis (Paper E). The platform described in Paper D is a hybrid approach, and the goal of the platform is to facilitate the impact of the ICT infrastructure on real world applications, which still requires real world ICT infrastructures, which, as mentioned earlier, is not practical. However, as illustrated in Publication V and Publication VI, real systems can be mixed with simulated systems to further improve prediction.

The rest of this section discusses simulation modeling and analysis and enterprise architecture modeling and analysis as a form of analytical modeling.
**SIMULATION MODELING AND ANALYSIS**

Simulation is applied in many fields ranging from the business domain to the military. A simple definition of simulation, found in [105], states that:

“Simulation is the imitation of the operation of the real-world process or system over time”.

Simulations duplicate real life phenomenon through the use of mathematical models. Simulations are therefore, models of a real life phenomenon that can be executed and observed on a computer system. Simulation models can be classified as follows:

- Discrete Simulation Models
- Continuous Simulation Models
- Combined Discrete Continuous Models

Discrete simulation is characterized by the fact that its variables change only at discrete points or events, for example, when a bank customer shows up at the teller, the teller will respond. The continuous simulation variables are always a subject to time, e.g., a queue of bank customers at the teller or how long will it take to serve the queue. Combined discrete-continuous simulations, as the name suggests, are a combination of both, where the simulation parameters are subject to time but also change according to discrete events that may occur during the course of the simulation. Simulations are used for product design, testing and training, among others, and are applied in such fields as manufacturing, the automobile industry, healthcare, the military, etc. [105].

Generally speaking, the parameters of simulation models can be more varied than those involved in analytical analysis. An example of a general purpose simulation package is OPNET [108], which can model many characteristics of communication networks. Especially targeting Power System Control, a set of simulators has been combined into a platform, for example, in [116], [132], [134]. In [116], for example, the EPOCH simulator is used to model different protection and control schemes, including power system and communication system characteristics.

Nevertheless, simulation models still cannot model every single detail of the system and involve assumptions and simplifications to implement the program and to execute it in a reasonable amount of time [107].

**SIMULATION PROCESS**

The simulation models implemented in this research are based on discrete event simulations. The OPNET Modeler [108] was used for Paper A and Paper B. OMNET++ [109] was also used in this work, specifically in Paper C. OMNET++ is similar in purpose and architecture to OPNET. The simulation models in Paper A used built-in and reusable models from the OPNET’s library. Most of the models were built on top of basic OPNET components using the propriety “C/C++-like” language of the simulator, called proto-C.

The steps in the method used for building the models in Paper A, B and C are illustrated in Figure 10. These steps are based on recommendations from [105] and [110].
The first step, establishes the need to build a simulation project by identifying a set of questions that a model should answer. These questions may arise from a literature review or from the results of previous research. The specification of the model in terms of characteristics, properties and behavior could also come from a literature review or from experts familiar with the characteristics and behavior of the physical or concept that is being modeled. In the case of the research in this thesis, the models were built to answer questions related to end-to-end delays and other data quality issues in wide area networks for WAMCs. This information is the basis for step 2, which involves the building of a preliminary model. The preliminary models are not necessarily sufficiently detailed to capture all properties of the real world concept being modeled but are sufficient to answer the questions or achieve the goal laid out in step 1.

The preliminary model is then validated in step 3 to establish its compliance with the input from literature, experts and/or the goal or question that was set at the start of the project. The validation may establish new aspects to correct or to add to the model. In step 4, the model is enhanced to meet the recommendations and findings from step 3. Finally, step 5 involves running the simulation, collecting results as statistics and analyzing the results.

**ENTERPRISE ARCHITECTURE MODELING AND ANALYSIS**

The EA analysis approach is a model-based approach, where an information system’s architecture and properties are captured in some sort of modeling language such as the Unified Modeling Language (UML) [111] or ArchiMate [113]. The resulting model of the system architecture and properties are then used to perform an analysis of that system from a specific nonfunctional quality viewpoint, for example, maintainability, availability, cyber security or interoperability. Unlike simulation modeling, this analytical modeling approach does not aim to mimic every property of the system under study but only the properties that are relevant for the desired viewpoint.

There has been extensive work in this area using several different but closely related methods. For example, in [45], traditional queuing-based quantitative analysis is applied to ArchiMate models for the analysis of performance in terms of utilization and response time. In [112], a Bayesian networks approach is used for the analysis of system maintainability. Probabilistic approaches such as those found in [49][50][51][52][112] are beneficial because they integrate into the analysis uncertainty about several aspects of the system, aspects related to data collected, i.e., the opinion of the user on the performance or the usability of the system or uncertainty in the architecture or properties of the system being modeled, for example, if a certain security protection measure exists in a certain subsystem.
The approach used in Paper E is similar to the aforementioned approaches and is based on the enterprise architecture analysis as described in [114]. The WAMM framework presented in Paper E captures a model of the system under study and applies an analysis framework to the models.

The models are captured using the UML, and the analysis is based on the Predictive, Probabilistic Architecture Modeling Framework (P²AMF) [53], an extension of the Object Constraint Language (OCL) [115]. OCL is a formal language used to define rules and invariants on UML models, and the language is capable of expressing first-order logic, arithmetic and set theory. P²AMF extends OCL by allowing the incorporation of uncertainty into the analysis. To illustrate how P²AMF is used, consider the simplified model illustrated in Figure 11.

A valid OCL statement describing the dependency relation between isdropped of the Dataflow class and the dropsMessage of the WAMC Component and Network Zone classes is as follows:

```
context Dataflow::isDropped: Boolean
derive: (self.medium>exists(dropsMessage)) or (self.server>exists(dropsMessage)) or (self.client>exists(dropsMessage))
```

The above OCL statement is also a valid P²AMF statement. The difference is as mentioned earlier that, in OCL, the values of dropsMessage for WAMC Component and Network Zone would be deterministic, i.e., in the case of the model in Figure 11, true or false. However, in P²AMF, these values are stochastic and defined as a probability distribution. Table 2 summarizes this difference.

<table>
<thead>
<tr>
<th>OCL</th>
<th>P²AMF</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAMC_Component::dropsMessage:Boolean init:true</td>
<td>WAMC_Component::dropsMessage:Boolean init:Bernoulli(0.3)</td>
</tr>
<tr>
<td>Network_Zone::dropsMessage:Boolean init:true</td>
<td>Network_Zone::dropsMessage:Boolean init:Bernoulli(0.2)</td>
</tr>
</tbody>
</table>
Apart from the attribute level uncertainty that P²AMF supports through a stochastic definition of attribute values, class level uncertainty can also be expressed. On the class level, uncertainty is expressed in terms of the existence of an instance and its relation. All classes and relations defined in P²AMF have an existence property. The existence attributed can be deterministic if the modeler is sure such an instance or its relations to other instances exist or they can be expressed probabilistically otherwise. An example of class level uncertainty is (in reference to the WAMM model in Paper E) the existence of a Zone Management Process for a certain scenario, or the existence of the same zone management process for another network zone.

Another aspect of P²AMF is the use of the Monte Carlo sampling technique for analyzing the model. Using the probabilistic values defined for classes, relations and attributes, the model can be sampled several times, and values for classes, relations and attributes in the model can be drawn from the respective defined probability distribution.

Figure 12 summarizes the EA analysis approach used as part of this research. The architecture meta model is defined with OCL-like P²AMF statements defining the classes and the relation to other classes, attributes and relation to other attributes, which is represented by the “Architecture Meta Model” in Figure 12. This Architecture Meta Model is used by the modeler to create instance models that represent a real world system. The instance model is then sent through the P²AMF (represented by the gears in Figure 12), which then performs a Monte Carlo sampling and executes the P²AMF statements defined in the Architecture Meta Model for each sample.

![Figure 12: EA Analysis process with P²AMF](image-url)
The P2AMF is implemented in the Enterprise Architecture Analysis Tool (EAAT) [54],[55]. The EAAT tool supports the creation of Architecture Meta-models (called Abstract models in the EAAT’s lingo) and the use of these Meta-models to create instance models. The framework described in Paper E, uses P2AMF and EAAT.

**SUMMARY**

The research in this thesis utilized a variety of data collection methods to build and validate models. Simulation was also used as the main analysis technique for these models. The advantage of using simulation is the reusability and extensibility of the models. Enterprise architecture analysis methods were also used to model non-functional quality aspects that were not suitably modeled in traditional discrete event simulations.
CHAPTER 4

RELATED WORKS

The research described in this thesis spans different fields and used different methods; therefore, there are numerous related works. This chapter presents the related works that are most directly relevant to this work. First, there are the works related to WAMC communication system architecture and simulation. Second, there are related works in the field of enterprise architecture.

There exists related work employing simulations for the evaluation of power system related ICT infrastructure or components, for example, in [116], [117], [118], [120], [121]. The related works discussed here are those that are similar to the simulation models built as part of this research and therefore those primary related to WAMC or PMU-based systems in general.

In [122], the data flows of NASPI's NASPInet network were simulated to determine communication bandwidth requirements, the impact of security mechanisms on the bandwidth and the end-to-end delays. The data flows originate from the PMUs and are sent to a PDC. The PDC forwards the data to a phasor data gateway (PDG) that acts as a publisher of PMU data, sharing and distributing PMU data to authorized subscribers. This model is implemented in the Network Simulator 2 (NS2)[123]. This work is also similar to the work in [124] but not with the intention of modeling the NASPInet network but rather generalized networks for the Western Interconnect grid in the USA and for the Polish Grid. In [125], an overview of WAMC architectures is presented with a discussion on the communication media and protocols that could be deployed. The goal of the work is to present a methodology for studying delays in WAMC systems. A characterization of a national WAMC system with 120 PMUs is implemented in OPNET, and several scenarios were created to model different WAMC application types, namely, power system monitoring, power system protection and power system control.

The aforementioned work is similar to that proposed in Paper A and specifically in the work leading up to Paper A, although it was done on a smaller number of PMUs. Furthermore, while paper A discusses the importance of requirements for various applications, it does not specifically implement scenarios for different application, as it is assumed that (with the absence of quality of service mechanisms) the underlying network architecture and properties would be the same. Furthermore, Paper A provides a comprehensive analysis of the delays with an application layer component (i.e., the PDC) and its contribution to the overall delay and data loss. The issue of data loss was further addressed in Paper C, which the preceding works did not address in their analysis. The work in this thesis and the methodology has been used as a basis for further simulation work in [126] and [127], where similar assumptions were made, albeit implemented in a different tool (NS2). The contribution of the latter work is an elaboration on different possible communication architectures for various types of power system applications, namely, monitoring, centralized control and decentralized control, while using different IP transport protocols (TCP and UDP).

The work in [77] and [128] is extremely important and interesting and considers an all-encompassing publish-subscribe overlay communication architecture for power system
real-time communication. This work and related simulation studies in [129] and [130] provide insight into an optimized, high performance, low latency network that guarantees quality of service for various types of applications. This architecture clearly accounts for ICT non-functional qualities in its design. The performance related work in this research in this thesis was not directed at proposing frameworks for power system communication but rather at analyzing the source of delays in WAMC systems and the implications of these delays, which is not directly and specifically addressed in such the aforementioned work.

There has also been some work on analyzing the impact of delays on application functions and on proposing methods for simultaneous analysis through co-simulation. In [131], the impact of delays on wide area control signals is discussed and illustrated. The authors use an analytical approach in which they assume the communication is in a series of M/M/1 queues over dedicated links. This study is extremely interesting and useful, but the network systems and conditions in the network systems are simplified and general and cannot be linked to conventional IP networks.

Another recent approach for analyzing ICT and power system interdependency is through combining simulations or co-simulation. In such approaches, a power simulator and communication simulator are usually integrated, and, in some cases, power system applications are added to the mix. These approaches have been outlined in [116],[132],[133],[134]. While such tools are extremely interesting and useful, their importance will increase because there is greater understanding on the interdependency of ICT and power systems. Nevertheless, most of this work has been demonstrative and not yet used for the specific analysis of delays or general non-functional quality attribute tradeoffs.

The use of enterprise architecture (EA) models supported by a formal framework for analysis is an approach to managing and optimizing complex ICT systems and processes. EA analysis methods have been applied in many scenarios, for example, in [45], [46], [47] and more specifically focusing on non-functional qualities of power system or utility ICT architectures, applications and processes in substation automation systems reliability [47], control system security [49] and interoperability[51].

In [45], queuing models and Little’s law are mapped to constructs in the ArchiMate language, allowing quantitative performance analysis of enterprise systems. In [135], a multi quality attribute framework for performance (response time), availability, data accuracy and application usage is presented, where the framework is built by adopting the ArchiMate meta-model and using P2AMF for the underlying analysis. While this framework supports multi quality attribute analysis, the framework does not directly model or include in the analysis the dependencies between the factors that impact these non-functional qualities as done in the case of WAMM with regard to the impact of security on interoperability.

The general purpose Interoperability Prediction Framework (IPF) described in [51] and the cyber security modeling language (CySeMoL) described in [52] are directly relevant to the Wide Area Monitoring and Control System Analysis Meta Model (WAMM) described in Paper E. WAMM directly specializes the concepts that are proposed in the interoperability modeling and prediction framework and therefore inherits its classes, relations and properties. WAMM then uses this basis to map and merge concepts from CySeMoL and attacks and countermeasures for these concepts. Thus, for example, a central concept in the IPF is the message-passing system, to which the network zone concept from the cyber security modeling language is mapped and merged, where the WAMM framework network zone concept contains relations and attributes inherited from both models.
The predictive depth of WAMM is equivalent to the IPF, but only a subset of the security aspects described in the CySeMol. CySeMol performs more extensive security analysis while, in WAMM, the primary importance is the dataflow. Therefore, WAMM focuses on attacks and counter-measures (and their dependent attacks and countermeasures) that aggregate on the dataflow. Furthermore, by integrating CySeMol with the interoperability and predication framework and specializing the model for Wide Area Monitoring and control systems, WAMM can show the impact of security on interoperability. This feature is in fact what also distinguishes WAMM from other analysis methods and techniques in the field.
CHAPTER 5

CONCLUSION

WAMC systems offer many opportunities to improve the real-time situational awareness in power systems. These systems are essentially SCADA systems but with continuous streaming measurement data. The quality of WAMC systems and the applications running on top of them are heavily, but not exclusively, dependent on the underlying ICT systems. The research explained in this thesis is a systematic approach to the analysis of WAMC ICT systems.

The heavy dependence on the ICT systems means that these systems should be viewed and treated as an integral component of WAMC systems. For example, delay problems cannot be merely solved by abstracting networks into clouds and throwing more bandwidth at them but rather a systematic understanding of how the underlying technologies function and what aspects need to be optimized. This understanding of the limitations on the optimizations needs should be integrated into the design of WAMC applications.

CONTRIBUTION

The contribution of this research can be summarized in the following points:

- Simulation based comparison and evaluation of communication architectures for WAMC systems. The research documented in this thesis addresses these paradigms by providing a comparison and evaluation through simulation and also provides insight on the impact of these architectures on the application level.

- Impact of the communication delays and components, specifically the PDC, on the overall data quality in WAMC systems. This research provides insight to the possible source(s) of delay in WAMC architecture and the impact of these delays on data quality, specifically data currency (the end-to-end delay of the phasor measurements) and data incompleteness, i.e., the percentage of the synchrophasor data lost in the communication.

- A probabilistic Monte-Carlo based framework for interoperability and cyber security modeling specialized for WAMC systems. The framework also captures possible impact of security on interoperability of WAMC data flows.

- A test bed where WAMC application and communication can be deployed and tested in a controlled but realistic environment.

FUTURE WORK

There are many possibilities to expand the research described in this thesis. Much work is still needed in the performance and data quality domain and the interoperability and cyber security domain. Of course, here are related non-functional qualities to consider, which are
equally as important but not investigated directly in this research, for example, reliability, availability and overlapping aspects such as scalability and survivability of WAMC systems. Interwoven in these possibilities is the need for frameworks, platforms and tools that can support decision making on the optimization and deployment of ICT and WAMC systems.

In regards to application requirements, non-functional quality attribute requirement specifications have to be investigated for different application profiles. Application profiles can be identified by grouping similar applications that have the same functional requirements. These profiles should then be subjected to further systematic analysis studies in terms of non-functional qualities to establish specific requirements in terms of robustness. Together with existing requirements, these would serve as non-functional reference models (as opposed to functional reference models). The importance of this work, in the author’s opinion, is paramount because technologies such as Gridstat [76], [77] or utilizing general quality of service mechanisms do not guarantee overall system quality if these specific technologies are not in turn tuned and optimized based on a utility’s application portfolio needs.

The interoperability and cyber security modeling and analysis framework described in this research could also be expanded. Currently, the framework can handle interoperability and aspects of cyber security, which can be improved by expanding the cyber security to account for more factors that influence security, such as social engineering or security related processes and procedures. Indications on how the model can be further specialized to represent specific WAMC components was discussed in this research, but an interesting extension would be more specific interoperability and security profiles for common components, which would naturally require more in-depth studies of each component and validation, possibly in a simulated laboratory experiment.

Integrating the analysis framework presented in this research to the platform would also be interesting, since that would add directly into the framework performance related issues and would serve as a basis for more in-depth analysis of the tradeoffs between cyber security, interoperability and performance.

Finally, other non-functional quality attributes such as reliability and availability should also be investigated because these attributes would also have an impact on the design of the ICT architecture and on the overall performance of WAMC systems.
BIBLIOGRAPHY


[90] Ullberg, J., Chen, D., Johnson, P., “Barriers to Enterprise Interoperability”. In the 2nd IFIP WG5.8 Workshop on Enterprise Interoperability, October 2009.


[99] Shepard, D.P., Humphreys, T.E., Fansler, A.A, Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks, International Journal of Critical Infrastructure Protection, Available online 1 October 2012,


PART II: PAPERS A TO E